IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please CANCEL claim 11 and AMEND claims 1, 2, 5, 6, 8, 9 and 12 in accordance with the following:

1. (Currently Amended) A file security management method, comprising:

obtaining a position in which a file can be opened as current position information from a position detecting device or as position information from an input device, and obtaining ~~data indicating~~ a number of high-order significant digits of the position information ~~used~~ for restricting a position of encryption or decryption of the file from the input device[[,]];

encrypting the file by using, as a key, data ~~having high-order digits corresponding to the number of significant digits~~ of the position information ~~obtained from the position information and the data indicating the number of significant digits~~ specified by the number of high-order significant digits;

further generating a first digest which is data resulting from a hash operation performed on the encrypted file, and generating public key encryption data by encrypting, using a public key, ~~the data indicating~~ the number of high-order significant digits, the file encrypted using the data of the position information specified by the number of high-order significant digits as a key, and the first digest; and

generating a second digest by performing a hash operation on the generated public key encryption data, and generating data to be provided by adding the second digest to the public key encryption data.

2. (Currently Amended) [[.]]A file security management method, comprising:

obtaining data to be provided having public key data which is generated by encrypting, using a public key, ~~data indicating~~ a number of high-order significant digits of position information, a file encrypted using data ~~corresponding to~~ of the position information specified by the number of high-order significant digits ~~of the position information~~, and a first digest obtained by performing a hash operation to the encrypted file, and a second digest obtained by performing a hash operation to the public key encryption data;

generating the data to be provided by adding the second digest to the public key encryption data;

generating a digest by performing a hash operation to the public key encryption data included in the data to be provided, and determining whether the generated digest matches the second digest included in the data to be provided;

decrypting, when the generated digest and the second digest matches, the public key encryption data using a secret key corresponding to the public key, and obtaining the ~~data indicating the~~ number of high-order significant digits ~~of the position information~~, the file encrypted using the data of the position information specified by the number of high-order significant digits and the first digest;

generating a digest by performing a hash operation to the obtained encrypted file, and determining whether the generated digest matches the obtained first digest; and

obtaining, when the generated digest and the first digest matches, current position information from a position detecting device, and performing a decryption process of the obtained encrypted file using data ~~having high-order digits corresponding to~~ of the current position information specified by the number of high-order significant digits ~~of the current position information~~ as a key.

Claims 3-4. (Cancelled)

5. (Currently Amended) A file security management apparatus, comprising:

an acquisition unit ~~for~~ obtaining a position in which a file can be opened as current position information from a position detecting device or as position information from an input device, and obtaining ~~data indicating~~ a number of high-order significant digits of the position information ~~used~~ for restricting a position of encryption or decryption of the file from the input device;

an encrypting unit encrypting the file by using, as a key, data of the position information ~~having high order digits corresponding to the significant number of digits of the position information obtained the position information and the data indicating~~ specified by the number of high-order significant digits; and

~~further~~ a generation unit generating a first digest which is data resulting from a hash operation performed on the encrypted file, and generating public key encryption data by encrypting, using a public key, the ~~data indicating the~~ number of high-order significant ~~digest~~

digits, the file encrypted using the data of the position information specified by the number of high-order significant digits as a key, and the first digest; and

data to be provided to the generation unit generating a second digest by performing a hash operation on the generated public key encryption data, and generating data to be provided by adding the second digest to the public key encryption data.

6. (Currently Amended) A file security management apparatus[[.]], comprising:

a first acquisition unit for obtaining data to be provided having public key data which is generated by encrypting, using a public key, ~~data indicating~~ a number of high-order significant digits ~~of position information~~, a file encrypted using the data of the position information ~~corresponding to~~ specified by the number of high-order significant digits ~~of the position information~~, and a first digest obtained by performing a hash operation to the encrypted file, and a second digest which is obtained by performing a hash operation to the public key encryption data; and generating the data to be provided by adding the second digest to the public key encryption data;

a first determination unit for generating a digest by performing a hash operation to the public key encryption data included in the data to be provided, and determining whether the generated digest matches the second digest included in the data to be provided;

a second acquisition unit for decrypting, when the generated digest and the second digest matches, the public key encryption data using a secret key corresponding to the public key, and obtaining ~~the data indicating~~ the number of high-order significant digits ~~of the position information~~, the file encrypted using the data of the position information specified by the number of high-order significant digits, and the first digest[[.]];

a second determination unit for generating a digest by performing a hash operation to the obtained encrypted file, and determining whether the generated digest matches the obtained first digest; and

a decryption unit for obtaining, when the generated digest and the first digest matches, current position information from a position detecting device, and performing a decryption process of the obtained encrypted file using data ~~having high-order digits corresponding to~~ of the current position information specified by the number of high-order significant digits ~~of the current position information~~ as a key.

7. (Cancelled)

8. (Currently Amended) A computer-readable storage medium on which a file security management program is recorded, the program which when executed by a computer causes the computer to perform a process comprising:

obtaining a position in which a file can be opened as current position information from a position detecting device or as position information from an input device, and obtaining ~~data indicating~~ a number of high-order significant digits of the position information ~~used~~ for restricting a position of encryption or decryption of the file from the input device[[,]];

encrypting the file by using, as a key, data ~~having high-order digits corresponding to the number of significant digits of the position information obtained from the position information and the data indicating~~ of the position information specified by the number of the high-order significant digits; and

further generating a first digest which is data resulting from a hash operation performed on the encrypted file, and generating public key encryption data by encrypting, using a public key, ~~the data indicating~~ the number of high-order significant digits, the file encrypted using the data of the position information specified by the number of high-order significant digits as a key, and the first digest; and encryption data, and generating data to be provided by adding the second digest to the public key encryption data.

9. (Currently Amended) A computer-readable storage medium on which a file security management program is recorded, the program comprising:

obtaining data to be provided having public key data which is generated by encrypting, using a public key, ~~data indicating~~ a number of high-order significant digits of position information, a file encrypted using data of the position information specified by ~~corresponding to~~ the number of high-order significant digits ~~of the position information~~, and a first digest obtained by performing a hash operation to be the encrypted file, and a second digest which is obtained by performing a hash operation to the public key encryption data; and generating the data to be provided by adding the second digest to the public key encryption data;

generating a digest by performing a hash operation to the public key encryption data included in the data to be provided, and determining whether the generated digest matches the second digest included in the data to be provided;

decrypting, when the generated digest and the second digest matches, the public key encryption data using a secret key corresponding the public key, and obtaining ~~the data indicating~~ the number of high-order significant digits ~~of the position information~~, the file encrypted

using the data of the position information specified by the number of high-order significant digits and the first digest;

generating a digest by performing a hash operation to the obtained encrypted file and determining whether the generated digest matches the obtained first digest; and

obtaining, when the generated digest and the first digest matches, current position information from a position detecting device and performing a decryption process of the obtained encrypted file using data of the current position information ~~having high-order digits corresponding~~ specified by the number of high-order significant digits ~~of the current position information~~ as a key.

Claims 10-11. (Cancelled)

12. (Currently Amended) The computer-readable medium of ~~claim 11~~ claim 8, wherein said encrypting includes encrypting the program with the position information and a license key given to a user.

13. (Cancelled)

14. (Previously presented) The computer-readable medium of claim 9, comprising:

receiving a program encrypted using position information and a license key, and

decrypting the encrypted program with position information which is detected by a position detecting device and the license key.

Claim 15-19 (Cancelled)

20. (Previously presented) The computer-readable storage medium according to claim 8, on which is recorded a program for reading map data from a storage medium on which is recorded map data encrypted with position information which specifies a position in which the map data can be used, the program including allowing the map data to be decrypted only if position information detected by a position detecting device and the position information used to encrypt the map data match.